CLAIMS

What is claimed is:

1. A method for ensuring the security of software in a computer system, comprising:

loading said software on said computer system;

validating said software by the use of a validator program;

marking said software as valid or invalid by the use of a digital signature flag; and,

denying access of said software to said computer system if said validator fails to identify said software as valid.

2. The method described in Claim 1 wherein said method operates on an open platform computer system.

3. The method described in Claim 1 wherein said method operates on a computer system which comprises:

a host computer; and,

a portable computing device coupled to said host computer.

4. The method described in Claim 1 wherein said software is supplied by a third-party source.

5. The method described in Claim 4 wherein said third-party software is for execution or other use on a palmtop computer.

6. The method described in Claim 1 wherein said validator program is specially constructed to reside in a secure fashion in said computer system.

7. The method Described in Claim 1 wherein said method operates on a computer system which comprises:

a network; and,

a palmtop computing device coupled to said network.

8. An apparatus for ensuring the security of software in a computer system, comprising:

a host computer;

a portable computing device coupled to said host computer; and,

a validation program.

9. The apparatus described in Claim 8 wherein said host computer is coupled to a network.

10. The apparatus described in Claim 8 wherein said portable computing device is a palmtop computing device.

11. The apparatus described in Claim 8 wherein said portable computing device is a personal data assistant.

12. The apparatus described in Claim 8 wherein said portable computing device is coupled to said host computer by an infrared device.

13. The apparatus described in Claim 8 wherein said portable computing device is coupled to said host computer by an RF enabled device.

14. The apparatus described in Claim 8 wherein said validation program resides in said host computer in a fashion intended to be secure.

15. The apparatus described in Claim 8 wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software if said third-party software is not found to be clean of known security compromising routines.

16. The apparatus described in Claim 15 wherein said palmtop computing device is configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached.

17. The apparatus described Claim 15 wherein said palmtop computing device is a Personal Data Assistant.

18. An apparatus for ensuring the security of software in a computer system, comprising:

a network;

a palmtop computing device coupled to said network; and,

a validation program.

19. The apparatus described in Claim 18, wherein said validation program resides in said computer network in a fashion intended to be secure.

20. The apparatus described in Claim 18, wherein said palmtop computing device is configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached.

21. The apparatus described in Claim 18, wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software if said third-party software is not found to be clean of known security compromising routines.

22. A portable computing device, comprising:

a bus;

a processor coupled to said bus;

volatile RAM coupled to said bus;

non-volatile ROM coupled to said bus;

a data storage device coupled to said bus;

an operating system, capable of storage on said data storage device or said non-volatile ROM or both and capable of special configuration;

a display coupled to said bus;

an alpha-numeric input device coupled to said bus;

a signal input/output device coupled to said bus; and,

a cursor control device coupled to said bus;

all of which are capable of operating under the control of said operating system software or firmware.

23. The portable computing device described in Claim 22 wherein said portable computing device is a palmtop computing device.

24. The portable computing device described in Claim 22 wherein said portable computing device is a personal data assistant.

25. The portable computing device described in Claim 22 wherein said portable computing device is capable of coupling with a host computer.

26. The portable computing device described in Claim 22 wherein said operating system is configured to load third-party applications and other files if said applications and other files are flagged by a validation program as being clean of security compromising routines.

27. The portable computing device described in Claim 25 wherein said coupling is enabled by an infrared device.

28. The portable computing device described in Claim 25 wherein said coupling is enabled by an RF device.

CONFIDENTIAL